4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/633,918	08/04/2003	Hamdy Soliman	NMTECH13.CIP2	4945

30996 7590 04/18/2007
ROBERT W. BECKER & ASSOCIATES
707 HIGHWAY 333
SUITE B
TIJERAS, NM 87059-7507

EXAMINER	
JACKSON, JENISE E	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/633,918	**Applicant(s)** SOLIMAN, HAMDY
	Examiner Jenise E. Jackson	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 February 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Guski et al(6,292,896).

3. As per claim 1, Guski et al. discloses a method of providing a secure data stream between system nodes(ref# 102, 104, fig. 1, sheet 1, col. 3, lines 48-57, fig. 3 sheet 2 and associated descriptions, col. 4, lines 26-32), providing a data record block(i.e. memory locations) including a plurality of data records within a predetermined interval(see col. 4, lines 1-15); providing a previous encryption key; (see col. 4, lines 26-32, 65-67); selecting an old data record from the plurality of data records; and regenerating a new encryption key at a user node as a function of the previous encryption key and the old data record(see col. 8, lines 59-67, col. 9, lines 1-4, 11-34, 44-50, col. 12, lines 17-43).

4. As per claim 2, Guski discloses wherein the step of selecting old data record includes selecting old data record using a byte from the previous encryption key as a seed of random generation (see col. 9, lines 25-67, col. 10, lines 1-13, col. 12, lines 17-43).

5. As per claim 3, Guski discloses wherein the step of regenerating the new encryption key includes regenerating a new encryption key by performing a logic operation on the previous encryption key and the old data record (see col. 9, lines 25-34, 44-50, col. 12, lines 17-43).

6. As per claim 4, Guski discloses wherein the step of regenerating the new encryption key by performing a logic operation includes regenerating the new encryption key by performing an XOR logic operation on the previous encryption key and the old data record (col. 9, lines 44-50).

7. As per claim 5, Guski discloses wherein the step of regenerating a new encryption key by performing a logic operation includes performing a logic operation on a previous encryption key and selected encrypted data to form an expanded key(see col. 9, lines 25-34, 52-58).

8. As per claim 6, Guski discloses the step of selecting bytes from the expanded key to generate the new encryption key(see col. 9, lines 25-58).

9. As per claim 7, Guski discloses wherein the step of selecting bytes from the expanded key to generate the new encryption key includes randomly selecting bytes from the expanded key to generate the new encryption key(see col. 9, lines 25-34).

10. As per claim 8, Guski discloses wherein the step of randomly selecting bytes from the expanded key to generate the new encryption key comprises randomly selecting bytes from the expanded key using a byte from the previous encryption key as a seed of random generation (see col. 9, lines 25-34, 59-65).

11. As per claim 9, Guski discloses the step of encrypting a new data record with the new encryption key forming a new encrypted data record(see col. 9, lines 25-34).

12. As per claim 10, Guski discloses wherein the step of encrypting the new data record with the new encryption key includes performing a logic operation on the new data record and the new encryption key(see col. 9, lines 25-34, 44-51).

13. As per claim 11, Guski discloses wherein the step of performing a logic operation on the new data record and the new encryption key includes performing an XOR operation on the new

data record and the new encryption key(see fig. 8 sheet 6, col. 9, lines 44-51).

14. As per claim 12, Guski discloses wherein the step of performing a logic operation on the new data record and the new encryption key includes forming a cipher(col. 9, lines 44-51).

15. As per claim 13, Guski discloses the step of permuting portions of the cipher to form another cipher(see col. 9, lines 44-51).

16. As per claim 14, Guski discloses the step of transmitting the new encrypted data record over a data stream(see fig. 3 sheet 2, col. 4, lines 26-32).

17. As per claim 15, Guski discloses the step of receiving the new encrypted data record at a destination node(see fig. 3 sheet 2, col. 4, lines 26-32).

18. As per claim 16, Guski discloses the step of decrypting encrypted data at the destination node(see col. 4, lines 65-67).

19. As per claim 17, Guski discloses wherein the step of decrypting the new encrypted data record includes decrypting the new encrypted data record with a previous decryption key forming a new decrypted data record (see col. 4, lines 26-32, 65-67).

20. As per claim 18, Guski discloses the step of regenerating a new decryption key as a function of the new decrypted data record and the previous decryption key, because Guski encryption/decryption key(session keys) are a key pair, and both nodes in Guski are synchronized with the same key(see col. 12, lines 17-27). Thus, when a new encryption key is regenerated the decryption key will be regenerated also(see col. 9, lines 25-34) .

21. As per claim 19, Guski discloses a system for providing a secure data stream between a source programmable apparatus and a destination programmable apparatus(see fig. 3, sheet 2),: a source programmable apparatus; a data stream created by said source programmable apparatus;

means for encrypting a data record of said data stream with a previous encryption key forming an encrypted data record(see col. 4, lines 26-32, 65-67); and means for regenerating a new encryption key using selected as a function of the previous encryption key and an old data record (see col. 9, lines 11-34, 44-50).

22. As per claim 20, Guski discloses a destination programmable apparatus in communication with said source programmable apparatus(see fig. 3 sheet 2); means for transmitting the encrypted data record to said destination programmable apparatus(see fig. 3 sheet 2); means for decrypting said encrypted data record received at said destination programmable apparatus with a previous decryption key forming a decrypted data record; and means for regenerating a new decryption key as a function of the previous decryption key and the decrypted data record(see col. 4, lines 26-32, 65-67, col. 9, lines 25-34, col. 12, lines 17-27).

Response to Amendment

23. A double patenting rejection was done in the office action 10/2/06. In Applicant's remarks filed 2/2/07, the Applicant has filed a terminal disclaimer in response to Examiner's double patenting rejection 10/2/06. The Applicant has amended claims 1-12, 14-20 filed 2/2/07.

24. The Applicant states that Guski does not disclose regenerating a new encryption key as a function of a previous encryption key and an old data record. The Examiner disagrees with the Applicant. Guski discloses a signon key is used as an encryption key for a DES encryption function to produce a 64-bit output block K. The 64-bit input block for DES encryption function is obtained by concatenating the 32-bit time/date value T with an additional value including the 32-bit right half of the second DES encryption product, which is derived from the secret signon

key K and the nonsecret signon information(see col. 8, lines 59-67, col. 9, lines 1-4). Guski discloses a session key is generated in the same manner at the authenticating node as the identical session key was at the requesting node, with the time value T being the regenerated value. The authenticating node copy of the signon key provides the key input to a DES encryption function to produce a output value K generated from the requesting node(see col. 12, lines 17-27). Values T and D2P1 are generated anew in response to the session key request(see col. 12, lines 29-43).

Final Action

25. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

April 14, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100